

# AQUILA - SonicWall Firewall Integration

This integration collects syslog messages from SonicWall firewalls. It has been tested with **Enhanced Syslog** logs from SonicOS versions 6.5 and 7.0, following the [SonicWall Log Events reference guide](#).

---

## Configuration

To set up the integration, configure a **Syslog Server** on your SonicWall firewall with the following settings:

- **Name or IP Address:**  
The address where your Elastic Agent (or AQUILA Agent) running this integration is reachable.
  - **Port:**  
The UDP port number for Syslog, matching the port configured in your integration.
  - **Server Type:**  
Select **Syslog Server**.
  - **Syslog Format:**  
Choose **Enhanced Syslog**.
  - **Syslog ID:**  
The default value is `firewall`. Change this if you want to differentiate logs from multiple firewalls. This value is stored in the `observer.name` field.
- 

## Time Configuration Recommendation

To avoid timestamp discrepancies:

- Enable **Display UTC in logs** in your SonicWall device under:  
`Device > Settings > Time Configuration`
  - If you use local time instead, configure the **Timezone Offset** setting in your integration to match your firewall's timezone.
- 

## Connectivity

Ensure proper network connectivity between your SonicWall firewall and the AQUILA Agent (or Elastic Agent) to receive syslog messages successfully.

*If you need further assistance, kindly contact our support at [support@cytechint.com](mailto:support@cytechint.com) for prompt assistance and guidance.*

---

Revision #2

Created 2 July 2025 12:08:42 by Richmond Abella

Updated 2 July 2025 12:51:05 by Richmond Abella